

## 明細書

## 眼画像入力装置および認証装置ならびに画像処理方法

## 技術分野

[0001] 本発明は、眼の画像を入力する眼画像入力装置およびそれを用いた認証装置および画像処理方法ならびにプログラムに関する。

## 背景技術

[0002] 近年、入退室管理装置や個人情報等の重要な情報が記憶された情報装置等、高いセキュリティ性が求められる装置におけるアクセス時の本人認証の方法として、人体の指紋、虹彩、眼底血管、顔の特徴、腕の血管パターン等、その被認証者固有のいわゆるバイオメトリクス情報を用いた様々な認証方法が実用化されてきている。

[0003] その中でも、本人認証率の高さや他人受入率の低さ等の信頼度の高さから、眼の虹彩部分の皺の模様の違いを利用した認証方法(以下、このような認証方法を虹彩認証方法と記す)が提案され、特に高いセキュリティ性が必要な機器において実用化されている(例えば、特許第3307936号公報を参照。)。

[0004] このような虹彩認証方法は、被認証者の眼画像から虹彩の部分を選択的にコード化し、得られた情報を認証情報として、あらかじめ登録された登録認証情報と比較照合し、互いに一致すると判定された場合には、被認証者があらかじめ登録された者であると認証する方法である。

[0005] このような虹彩認証方法を用いた認証装置も様々な形態のものが提案されていている。その一例として、被認証者の眼画像を撮影するカメラを搭載したハンディ型の眼画像入力装置をコンピュータ等の情報装置に外付けで接続し、眼画像入力装置から入力された眼画像を情報装置側でコード化処理および比較照合処理して被認証者の認証を行う構成の認証装置が提案されている(例えば、特開2000-207536号公報を参照。)。

[0006] このような認証装置においては、眼の虹彩部分が鮮明に撮影された眼画像を得るために、情報装置の表示部の画面上に眼画像入力装置で撮影された眼画像を所定の位置に誘導するための画像として表示し、被認証者はその眼画像を見ながら適切

な眼が撮影される位置に眼画像入力装置を移動させて眼画像を撮影する構成であった。

- [0007] しかしながら、前述したような認証装置においては、情報装置の画面に眼画像入力装置で撮影された眼画像が表示されるので、表示された眼画像を画面コピーする等して複製することによって、眼画像が不正に取得される可能性があった。
- [0008] これにより眼画像が不正に取得された場合には、取得した眼画像を利用した第三者が登録された者として認証を受けてしまう、いわゆる「なりすまし」が行われる可能性があるという課題があった。

### 発明の開示

- [0009] 本発明はこのような課題に鑑みてなされたもので、表示部の画面に表示された画像を不正に取得されても、いわゆる「なりすまし」の行われる可能性の低い、セキュリティ性の高い眼画像入力装置およびそれを用いた認証装置および画像処理方法ならびにプログラムを提供することを目的とする。
- [0010] 本発明の眼画像入力装置は、眼画像が入力される眼画像入力部と、眼画像の少なくとも虹彩を含む部分の画像を劣化させて眼画像の表示画像を作成する表示画像作成部と、表示画像作成部で作成された表示画像を表示する表示部とを備えたことを特徴としている。
- [0011] このような構成により、表示部に表示された画像を不正に取得されても、画像の虹彩を含む部分の画像が劣化しているので、不正な者があらかじめ登録された者になりますための画像の取得の可能性の低い、セキュリティ性の高い眼画像入力装置を提供できる。
- [0012] 次に、本発明の認証装置は、前述の眼画像入力装置と、眼画像入力部から入力された被認証者の眼画像から、認証情報を作成する認証情報作成部と、認証情報とあらかじめ登録された登録認証情報を比較照合することにより、被認証者の認証を行う認証部とを備えたことを特徴としている。
- [0013] このような構成により、表示部に表示された画像を不正に取得されても、画像の虹彩を含む部分の画像が劣化しているので、不正な者があらかじめ登録された者になりますという可能性の低い、セキュリティ性の高い認証装置を提供できる。

- [0014] また、表示画像作成部は、被認証者の眼位置誘導に使用する表示画像を作成し、認証情報作成部は、表示部の表示画像によって所定の位置または領域まで誘導された被認証者の眼画像から認証情報を作成する構成であってもよい。
- [0015] このような構成によれば、さらに、眼画像入力部に対する被認証者の眼の位置を誘導する際に表示する表示画像の虹彩を含む部分の画像を劣化させることができるので、誘導の際に表示される画像を複写等して、それを用いて認証を行おうとしても排除される可能性が高くなることから、表示部に誘導用の画像を表示して被認証者の誘導を行う認証装置において、セキュリティ性の高い構成を実現できる。
- [0016] また、被認証者の眼画像から作成された認証情報を登録認証情報として登録する認証情報登録部を備え、表示画像作成部は、被認証者の眼画像の登録の可否を判定させるための表示画像を作成し、認証情報登録部は、表示画像作成部で作成された表示画像を表示部に表示させてから認証情報を登録認証情報として登録する構成であってもよい。
- [0017] このような構成によれば、さらに、被認証者の眼画像から作成した認証情報を登録認証情報として作成する場合に、前もって確認用の画像を表示する認証装置において、セキュリティ性の高い構成を実現できる。
- [0018] さらに、表示画像作成部は、眼画像の少なくとも虹彩を含む部分を選択的に画像処理して表示画像を作成する構成であってもよい。
- [0019] このような構成によれば、さらに、認証情報の作成に際して必要な虹彩を含む部分を選択的に画像処理することにより、全体の演算量を減らして装置の低コスト化および演算の迅速化を図ることが可能となる。
- [0020] また、認証情報作成部は、眼画像から眼の位置を検出する眼位置検出部と、眼画像から瞼の位置を検出する瞼位置検出部とを有し、表示画像作成部は、眼の位置および瞼の位置から眼画像の少なくとも虹彩を含む部分の位置を特定し、選択的に画像処理を行う構成であってもよい。
- [0021] このような構成によれば、さらに、認証装置が眼画像から認証情報を作成する際に用いる眼位置および瞼位置の情報を利用して、眼画像を切出して、それから少なくとも虹彩を含む部分を選択的に処理することが可能となり、別途眼位置検出や瞼位置

検出を行う必要がなく、装置の簡易化および処理の迅速化を図ることが可能となる。

- [0022] また、表示画像作成部は、眼画像を圧縮処理することによって表示画像を作成する構成であってもよい。
- [0023] このような構成によれば、さらに、画面コピー等が行われても容易にはなりすまし等の不正行為を行うことのできないセキュリティ性の高い構成を実現できる。
- [0024] さらに、圧縮処理がJPEG圧縮処理である構成であってもよい。
- [0025] このような構成によれば、さらに、広く知られた圧縮アルゴリズムによって、被認証者に対しての眼位置誘導に使用することができるものの、認証に使用するには極めて困難な画質の表示画像とすることができます、セキュリティ性の高い表示画像を作成することが可能となる。
- [0026] また、表示画像作成部は、眼画像を構成する画素列の間引き処理によって表示画像を作成する構成であってもよい。
- [0027] このような構成によれば、さらに、画面コピー等が行われても容易にはなりすまし等の不正行為を行うことのできないセキュリティ性の高い構成を実現できる。
- [0028] また、表示画像作成部は、眼画像に所定のノイズを付加する処理によって表示画像を作成する構成であってもよい。
- [0029] このような構成によれば、さらに、画面コピー等が行われても容易にはなりすまし等の不正行為の行われないセキュリティ性の高い構成を実現できる。
- [0030] さらに、表示画像作成部は、眼画像を構成する画素列の間引き処理、眼画像の圧縮処理、および、眼画像に所定のノイズを付加する処理のうち少なくとも2つを組み合わせた処理を行って表示画像を作成する構成であってもよい。
- [0031] このような構成によれば、さらに、画面コピー等が行われても容易にはなりすまし等の不正行為の行われない、かつ、見た目に自然な表示画像を表示できる構成を実現できる。
- [0032] また、表示画像作成部は、眼画像の少なくとも虹彩を含む部分と所定の画像との置換処理によって表示画像を作成する構成であってもよい。
- [0033] このような構成によれば、さらに、画面コピー等が行われても容易にはなりすまし等の不正行為の行われる可能性の極めて低い、セキュリティ性の高い構成を実現できる。

[0034] また、眼画像入力部に入力された眼画像の画質の良否を判定する画質判定部を備え、認証情報作成部は、画質判定部において画質が良いと判定された眼画像について認証情報を作成する構成であってもよい。

[0035] このような構成によれば、さらに、被認証者の眼画像のうち良い画質の眼画像から認証情報を作成できるので、認証率の高い認証情報を作成することが可能となる。

[0036] 次に、本発明の認証装置は、被認証者の眼画像が入力される眼画像入力部と、被認証者の眼画像から認証情報を作成する認証情報作成部と、認証情報を登録認証情報として登録する認証情報登録部と、認証情報とあらかじめ登録された登録認証情報とを比較照合することにより、被認証者の認証を行う認証部と、眼画像の少なくとも虹彩を含む部分の画像を劣化させて表示画像を作成する表示画像作成部と、表示画像を表示する表示部とを備え、表示画像作成部は、被認証者の誘導を行う場合および認証情報登録部が認証情報を登録認証情報として登録する場合の少なくともいずれかの場合に表示画像を作成して表示部に表示させることを特徴としている。

[0037] このような構成によれば、被認証者を誘導する場合および認証情報を登録認証情報として登録する場合のいずれの場合にも、画面コピー等が行われても容易にすまし等の不正行為の行われる可能性の極めて低い表示画像を用いでるので、セキュリティ性の高い構成を実現できる。

[0038] 次に、本発明の画像処理方法は、眼画像から少なくとも虹彩を含む領域を切出す第1のステップと、第1のステップで切出された領域の画像を選択的に劣化させる処理を行う第2のステップとを備えたことを特徴としている。

[0039] このような方法によれば、画像を不正に取得されても、画像の虹彩を含む部分の画像が劣化しているので、不正な者があらかじめ登録された者になりすまして認証を受ける可能性の低い、セキュリティ性の高い画像処理方法を実現できる。

[0040] 次に、本発明のプログラムは、コンピュータに、眼画像から少なくとも虹彩を含む領域を切出す第1のステップと、第1のステップで切出された領域の画像を選択的に劣化させる処理を行う第2のステップとを実行させることを特徴としている。

[0041] このようなプログラムにより、画像を不正に取得されても、画像の虹彩を含む部分の画像が劣化しているので、不正取得者があらかじめ登録された者になりすまして認証

を受ける可能性の低い、セキュリティ性の高い画像処理を行えるプログラムを実現できる。

[0042] 以上述べたように、本発明によれば、表示部に表示された画像を不正に取得されても、画像の虹彩を含む部分の画像を認証に使用できないよう劣化させているので、不正取得者があらかじめ登録された者になります可能性の低い、セキュリティ性の高い眼画像入力装置および認証装置および画像処理方法ならびにプログラムを提供できる。

#### 図面の簡単な説明

[0043] [図1]図1は、本発明の第1の実施の形態における認証システムの概要を説明する図である。

[図2]図2は、本発明の第1の実施の形態における認証装置1の構成を示すブロック図である。

[図3]図3は、本発明の第1の実施の形態における認証装置1の処理ステップを示すフローチャートである。

[図4]図4は、本発明の第1の実施の形態における表示画像の一例を示す図である。

[図5]図5は、本発明の第1の実施の形態における表示画像の他の例を示す図である。

[図6]図6は、本発明の第1の実施の形態における表示画像のさらに他の例を示す図である。

[図7]図7は、本発明の第1の実施の形態における表示画像のさらに他の例を示す図である。

[図8]図8は、本発明の第1の実施の形態における認証機能を有する携帯電話装置の外観を示す図である。

[図9]図9は、本発明の第2の実施の形態における認証システムの概念を示す図である。

[図10]図10は、本発明の第2の実施の形態における認証システムの構成を示すブロック図である。

[図11]図11は、本発明の第2の実施の形態における認証システムの動作ステップを

示すフローチャートである。

[図12]図12は、本発明の第3の実施の形態における認証システムの構成を示すブロック図である。

[図13]図13は、本発明の第3の実施の形態における表示画像の一例を示す図である。

[図14]図14は、本発明の第3の実施の形態における表示画像の他の例を示す図である。

[図15]図15は、本発明の第3の実施の形態における表示画像のさらに他の例を示す図である。

[図16]図16は、本発明の第4の実施の形態における認証システムの構成を示すブロック図である。

[図17]図17は、本発明の第5の実施の形態における認証システムの構成を示すブロック図である。

#### 符号の説明

- [0044] 1, 61, 75 認証装置
- 2, 62, 82 画像入力部
- 3 画質判定部
- 4 眼位置検出部
- 5 瞼位置検出部
- 6 極座標変換部
- 7 コード化部
- 8 照合部
- 9 記憶部
- 10, 20 登録部
- 11, 31, 71, 81, 94 表示画像作成部
- 12, 72, 83 表示部
- 13, 84 入力部
- 21 被認証者

- 22, 63 情報伝達部
- 23 管理者
- 30, 60, 70, 85, 88 認証システム
- 40 携帯電話装置
- 41 LED
- 42 ダイレクトキー
- 43 CCDカメラ
- 44 液晶ディスプレイ
- 50~54, 80, 91~93 表示画像
- 64 登録管理装置
- 65 眼位置誘導部
- 66 鏡誘導部
- 67 移動指示部

#### 発明を実施するための最良の形態

- [0045] 以下、本発明の実施の形態について、図面を用いて詳細に説明する。
- [0046] (第1の実施の形態)
  - まず、本発明の第1の実施の形態である認証システムについて説明する。
- [0047] 図1は、本発明の第1の実施の形態における認証システムの概要を説明する図である。
- [0048] 図1において、本発明の第1の実施の形態における認証システム30は、被認証者21の眼を含む領域の画像(以下、眼画像と記す)を入力する画像入力部2、画像入力部2で入力された眼画像の虹彩領域を後述する方法で認証情報にコード化し、あらかじめ登録された登録認証情報と比較照合を行うことによって、被認証者21があらかじめ登録された者であるか否かの認証を行う認証装置1、および、被認証者21の眼画像を後述する方法で画像処理することにより作成された表示画像50を表示する表示部12を備えている。
- [0049] 画像入力部2としては、公知のCCDカメラ等の撮影装置を用いることができる。
- [0050] 画像入力部2と認証装置1とは情報伝達部22で接続されており、画像入力部2で

撮影された画像情報は、認証装置1に送られる。なお、情報伝達部22は、有線ケーブルであってもよいし、無線や赤外線等の公知の通信手段から任意に選択することが可能である。

- [0051] 表示部12としては、液晶やEL等を用いた公知の表示装置から任意に選択することが可能である。
- [0052] このような認証システム30を用いて、被認証者21は、まず、画像入力部2を手に持ち、画像入力部2は被認証者21の一方の眼の撮影を連続的に行う。撮影された画像は、情報伝達部22を通して認証装置1に送られる。認証装置1では、画像入力部2から入力された画像が、後述する方法によって表示画像50に画像処理されて表示部12に表示される。
- [0053] 被認証者21は、画像入力部2を動かしながら、一方の眼を撮影し他方の眼で表示部12に表示された表示画像50を見て、適切な位置(例えば表示部12の中央または表示されたガイド内)に眼が誘導された場合に、画像入力部2または認証装置1に設けられた入力部(図示せず)に認証を開始する旨の入力を行うことで、被認証者21が選択した眼画像が認証装置1に取りこまれる。
- [0054] 認証装置1においては、取りこまれた眼画像を用いてその虹彩領域を切り出し、例えば前述した特許第3307936号公報に記載された方法で認証処理を行い、被認証者21があらかじめ登録された者として認証されたか否かの信号を外部装置、例えば表示部12に出力する。このようにして、認証システム30を用いることにより、被認証者21の眼の虹彩パターンを用いて、被認証者21があらかじめ登録された否かの認証を行うことが可能となる。
- [0055] 本発明の第1の実施の形態の認証システム30においては、被認証者21が表示部12に表示された表示画像50を見ながら自ら画像入力部2の位置を移動させること、すなわち表示画像50を誘導に用いることによって、認証に必要な虹彩領域を含む眼画像を適切に認証装置1に取りこむことが可能となる。
- [0056] 次に、本発明の第1の実施の形態における認証システム30が備える認証装置1について、さらに詳しく説明する。図2は、本発明の第1の実施の形態における認証装置1の構成を示すブロック図である。

[0057] 図2において、本発明の第1の実施の形態における認証装置1は、入力された画像から後述する表示画像を作成して出力する表示画像作成部11、同じく入力された画像の画質の良否を判定する画質判定部3、画質判定部3で画質が良いと判定された画像についてその画像から撮影された眼の位置を検出する眼位置検出部4、同じく画像から撮影された瞼の位置を検出する瞼位置検出部5、画像の座標を極座標変換する極座標変換部6、極座標変換された情報を所定の方法でコード化して、認証情報を作成するコード化部7、コード化された認証情報のうち、登録すべき情報を登録認証情報として登録する登録部10、登録認証情報を記憶する記憶部9、および、画像からコード化部7でコード化された認証情報と記憶部9に記憶された登録認証情報を所定の方法で比較照合することにより互いに一致すると判定された場合に認証可能である旨の認証結果の出力を行う照合部8を備える。

[0058] なお、眼位置検出部4、瞼位置検出部5、極座標変換部6、コード化部7および照合部8それぞれの機能に関しては、例えば前述の特許第3307936号公報に提案された方法を用いて実現することができる。

[0059] 画質判定部3では、画像入力部2から入力された画像について、そのコントラスト等の画質評価項目が所定の範囲内にあるか、および、画像中に眼が撮影されているか否か等が判定される。

[0060] 記憶部9は、半導体メモリや磁気ディスク等の公知の記憶装置から任意に選択して用いることが可能である。

[0061] なお、画質判定部3、眼位置検出部4、瞼位置検出部5、極座標変換部6、コード化部7、照合部8、登録部10および表示画像作成部11の機能は、それぞれがハードウェアで実現されてもよいし、それぞれの機能がソフトウェアで実現可能に記述され、演算装置等で実行される構成であってもよい。このようにそれぞれの機能がソフトウェアによって実現されている場合には、上記の各機能ブロックを実現するプログラムを演算装置にロードしたコンピュータを用いて認証装置1を構成することが可能となる。

[0062] 次に、本発明の第1の実施の形態における認証装置1の動作について説明する。図3は本発明の第1の実施の形態における認証装置1の処理ステップを示すフロー

チャートである。

- [0063] まず、画像入力部2が撮影した眼画像が、表示画像作成部11に入力される(S1)。
- [0064] 表示画像作成部11は後述する方法で、表示画像50を作成(S2)する。次に、表示部12に対して表示画像作成部11は表示画像50を出力し、表示部12は表示画像50を表示する(S3)。
- [0065] 被認証者21は、前述のように自らの眼画像を誘導に用いて、表示画像50が表示部12上の所定の位置(例えば画面の中央部)に表示されているかを判定し、正しい位置に表示されている場合には、誘導完了の入力を行う(S4)。
- [0066] 被認証者21からの入力があった場合(S5)には、画質判定部3が画質の判定を行い(S6)、画質が良いと判定された場合には(S7)、画像は画質判定部3から眼位置検出部4に送られ、以降の認証処理または必要に応じて被認証者21を認証可能な者として登録する登録処理(S8)が行われる。認証処理や登録処理の具体的な内容については、例えば前述の特許第3307936号公報に記載された方法を用いることができる。
- [0067] 一方、ステップS7において、画質判定部3で画質が悪いと判定された場合には、表示部12に対してエラーメッセージを表示させる等により、被認証者21に対して再度画像を撮影する旨を通知する(S1)。
- [0068] ここで、表示画像作成部11で作成される表示画像50について、詳細に説明する。
- [0069] 表示画像作成部11においては、万が一不正な行為、すなわち表示部12において表示される表示画像50が画面コピーされたりした場合においても、その画像を用いて第三者が被認証者21になりすまして認証を受ける等の不正行為を容易に行えないような表示画像を作成する必要がある。すなわち、表示画像作成部11は、鮮鋭な眼画像を劣化させることによって表示画像50を作成する。ここで、眼画像を劣化させると、コントラスト、明るさ、ピント等のあった鮮鋭度の高い眼画像のうち、虹彩の領域から認証情報を作成できないように、または作成しても元の鮮鋭度の高い眼画像から作成された認証情報と一致しない程度にまでその画質を低下させる、または後述するように眼画像の一部分または全部を別の画像に置換することをいう。
- [0070] このような処理を実現するための一例として、表示画像作成部11は、入力される画

像をその周波数領域によって圧縮する方法、例えば、広く知られたJPEG (Joint Photographic Experts Group) 方式で圧縮することによって表示画像50を作成することができる。JPEG圧縮処理することにより、表示画像50を用いてなりすましされる可能性を著しく低減することが可能となる。

- [0071] なお、ここでJPEG圧縮処理とは、例えば、ダウンサンプリング、DCT (Discrete Cosine Transform: 離散コサイン変換) 処理、量子化処理およびHuffman変換を行うことで実現できるが、この方法以外にも、例えばDCT処理をDWT処理 (Discrete Wavelet Transform: 離散ウェーブレット変換) 処理に置き換える等、公知の様々な方法を用いることができる。
- [0072] このようなJPEG圧縮された表示画像51の例を図4に示す。表示画像51の圧縮率は98%である。図4に示したように、表示画像51は虹彩パターンがほぼ見分けられないほどに圧縮されており、なりすましに用いられる可能性を著しく低減することを可能とする。なお、ここで圧縮率とは、圧縮処理前後の画像情報の大きさ(バイト数)の比率であり、  

$$\text{圧縮率} = 100 - (\text{圧縮後の画像サイズ} / \text{元画像サイズ}) \times 100$$
 で表される。
- [0073] 検討によれば、見た目に不自然さを感じにくく、かつ、画面コピーによるなりすましを防ぐためには、その圧縮率を一定の範囲にすることが望ましい。
- [0074] 圧縮率が高すぎると見た目に不自然さを感じ、圧縮率が低すぎると画面コピーされたような場合になりすましされる可能性が発生する。上述した図4の画像によれば、表示画像51を用いて効果的に、かつ違和感を覚えさせることなく自然に被認証者21を誘導することが可能である。
- [0075] また、別 の方法として、表示画像作成部11で画像を構成する画素の間引き処理(以下、リサイズと記す)を行うことにより、なりすましされる可能性を低減することが可能である。一例として、行方向および列方向にそれぞれ19画素おきに間引いて作成した表示画像52を図5に示す。図5に示したように、表示画像52も虹彩パターンがほぼ見分けられず、なりすましに用いられる可能性を著しく低減することが可能となる。また、この場合にも、表示画像52を用いて効果的に、かつ違和感を覚えさせることなく

自然に被認証者21を誘導することが可能である。

- [0076] なお、本発明においては、このリサイズの方法を限定するものではないが、例えば、縦横それぞれ1ラインおきに画素を間引く等の方法を行うことが可能であるし、縦方向または横方向のみ間引き処理を行うことも可能である。
- [0077] さらに、別 の方法として、表示画像作成部11で画像に対してノイズ情報を付加する処理を行うことによって表示画像53を作成してもよい。本発明においては、このノイズ付加の方法を限定するものではないが、一例として、ランダムに輝度振幅50のノイズ信号を発生し、そのノイズ信号を各画素毎の輝度に加減算して作成した表示画像53を図6に示す。図6に示したように、表示画像53も虹彩パターンがほぼ見分けられないほどに画像が劣化しており、なりすましに用いられる可能性を著しく低減することが可能となる。また、この場合にも、表示画像53を用いて効果的に、かつ違和感を覚えさせることなく自然に被認証者21を誘導することが可能である。
- [0078] なお、本明細書においては、説明を簡単にするために、画像を構成する各画素の輝度階調は全て256階調であるとする。
- [0079] なお、このノイズ付加の方法としては、前述のようにランダムに発生させたノイズを付加する他にも、例えば、所定の振幅のガウス分布に従ったノイズを発生して、そのノイズを付加することも可能である。
- [0080] さらに、上述の圧縮、リサイズおよびノイズ付加のうち2つ以上の処理を組み合わせて表示画像54を作成してもよい。図7にこのような表示画像54の一例を示す。
- [0081] 図7に示した表示画像54は、縦方向に4分の1、横方向に4分の1にそれぞれリサイズして、さらにJPEG圧縮処理(圧縮率95.6%)を行ったものである。
- [0082] このように作成した表示画像54は、図7に示したように自然な眼画像であり被認証者21に不快感を与えるにくく、かつ、認証に用いる虹彩の皺模様が不明確であるために、この表示画像54をなりすましに用いられる可能を極めて低くすることが可能である。
- [0083] 以上述べたように、本発明の第1の実施の形態における認証システム30を用いることにより、被認証者21の誘導等に用いるために表示部12に表示させる表示画像50を所定の方法によって作成することにより、表示部12の画面コピー等が行われた場

合にも、なりすましのされにくい、セキュリティ性の高い認証システムを提供できる。かつ、表示画像50を用いて効果的に、かつ違和感を覚えさせることなく自然に被認証者21を誘導することも可能である。

- [0084] なお、本発明の第1の実施の形態における認証システム30においては、被認証者21がその画像入力部2を手で移動させる例を示したが、本発明はこれになんら限定されるものではない。例えば、画像入力部2が据え置きされており、被認証者21が自らの眼の位置を動かして適切な眼画像を撮影する構成であってもよいことはいうまでもない。
- [0085] また、本発明の第1の実施の形態の認証システム30においては、画像入力部2、認証装置1および表示部12が別々の機器として構成された例を示したが、本発明はこれになんら限定されるものではない。例えば、画像入力部2が認証装置1に組み込まれていたり、表示部12が認証装置1に組み込まれていたり、画像入力部2と表示部12とが一体に構成されていたり、さらには、画像入力部2、認証装置1および表示部12が一体に構成されていてもよいことはいうまでもない。
- [0086] 例えば、画像入力部2、認証装置1および表示部12が一体に構成された認証システムの例として、認証機能を有する携帯電話装置40の外観を図8に示す。
- [0087] 図8に示した携帯電話装置40は、前述した画像入力部2としてCCDカメラ43を備え、表示部12として液晶ディスプレイ44を備えている。
- [0088] さらに、携帯電話装置40は、被認証者21の虹彩の高コントラストな画像を撮影するために、赤外線を発生する2つのLED41を備えている。また、前述のCCDカメラ43は可視光カット(赤外透過)フィルタを有しており、被認証者21の虹彩の高コントラストな画像を撮影できる。なお、LED41を2つ備えた理由は、被認証者21が眼鏡をかけているような場合に、いずれか一方の光源を用いて撮影した画像には眼鏡のレンズ等における反射光が含まれない可能性が高いため、すなわちこのような構成により、眼鏡反射光成分を除去するためである。
- [0089] 被認証者21は、液晶ディスプレイ44に表示された表示画像50を見ながら、自らの眼が適切に表示された場合(例えば、画面の中心に欠けることなく表示された場合、または別途設けられたガイド部に適応した表示がされた場合)に所定のダイレクトキ

ー42を押すことにより、眼画像が、携帯電話装置40に内蔵された認証装置1に入力され、被認証者21の認証を行うことが可能となる。

[0090] さらに、本発明の第1の実施の形態の認証システム30においては、被認証者21が自らの眼の近傍に画像入力部2を移動させて撮影する例を示したが、本発明はこれに限定されない。例えば、被認証者21は、画像入力部2よって自らの眼を含む広角領域(例えば顔全体や体全体等)を撮影し、認証装置1は画像から眼の領域を適切に切出して認証処理に供する構成であってもよいことはいうまでもない。

[0091] (第2の実施の形態)

次に、本発明の第2の実施の形態における認証システムについて説明する。

[0092] 図9は、本発明の第2の実施の形態における認証システムの概念を示す図である。

[0093] 図9に示したように、本発明の第2の実施の形態における認証システム70は、被認証者21の眼画像が入力される画像入力部62と、画像入力部62に情報伝達部63を介して接続された登録管理装置64とを備える。

[0094] さらに、登録管理装置64は、認証装置61、表示部72および入力部13を有する。

[0095] このような認証システム70の形態は、一般的に被認証者21の入退室を管理する入退室管理システムに広く用いられている。入退室管理システムにおいては、あらかじめ被認証者21の眼画像を撮影して、そのコード化された認証情報を登録認証情報として登録する処理を行うとともに、被認証者21が入室または退室する場合に、被認証者21の眼画像を撮影し、被認証者21の眼画像から作成した認証情報と登録された登録認証情報を比較照合して、被認証者21があらかじめ登録された者であると認証された場合に入室または退室を許可する処理を行う。

[0096] このうち、被認証者21を以降認証可能な者として登録処理する場合に、本発明の第2の実施の形態における認証システム70においては、被認証者21は画像入力部62で自らの眼画像を撮影して、遠隔に配置された登録管理装置64において、管理者23がその眼画像を目視により確認して、その眼画像を登録してよい画像であると判定した場合には、その眼画像を登録画像として登録する。すなわち、管理者23は、表示部72に表示された眼画像を見て、眼が十分見開かれているか(十分な虹彩領域が確保されているか)、眼の虹彩を含む領域が画面内に入っているか等を目視で

確認して、問題がなければ登録許可する。

- [0097] このような入退室管理システムにおいては、従来から、管理者23が不正な目的で登録管理装置64の表示部72に表示された眼画像を画面コピーする等して複製することによって、その眼画像を用いてなりすましを行う可能性が指摘されてきた。
- [0098] しかしながら、本発明の第2の実施の形態における認証システム70においては、表示部72に表示される表示画像80は後述する方法で画像処理されて作成されているので、複製してもなりすまし等を行うことができない。
- [0099] 図10は、本発明の第2の実施の形態における認証システム70の構成を示すブロック図である。
- [0100] 図10に示した認証システム70における認証装置61の機能ブロックのうち、第1の実施の形態に示した認証装置1の機能ブロックと共通する部分については同一の符号を付して、その説明を省略する。
- [0101] 本発明の第2の実施の形態における認証装置61が第1の実施の形態に示した認証装置1と異なるところは、画像入力部62から眼画像が表示画像作成部31に入力されるのではなく、登録部20から表示画像作成部31へ眼画像が送られること、および、登録部20に管理者23が操作する入力部13からの信号が入力されることである。
- [0102] また、本発明の第2の実施の形態における画像入力部62が第1の実施の形態における画像入力部2と異なるところは、画像入力部62が被認証者21を誘導するための眼位置誘導部65を備えていることである。なお、眼位置誘導部65は、被認証者21が自らの眼が映る位置に移動することにより、装置に対して水平および垂直方向の誘導を行う鏡誘導部66、および、被認証者21が装置との距離を適当に調節できるように、被認証者21が移動すべき方向を音声や画像等で指示する移動指示部67を有する例を図9に示す。
- [0103] 以下、認証システム70の動作について説明しながら、本発明の第2の実施の形態における認証装置61と第1の実施の形態に示した認証装置1との違いを詳細に説明する。
- [0104] 図11は、本発明の第2の実施の形態における認証システム70の動作ステップを示すフローチャートである。以下、被認証者21を登録する際の動作について説明する

[0105] まず、画像入力部62において、被認証者21の眼画像が撮影される(S10)。この場合、画像入力部62に搭載された眼位置誘導部65によって、被認証者21は負担を感じことなく自らの眼を撮影することが可能である。

[0106] 次に、撮影された眼画像は画質判定部3に送られて、前述したような画質判定が行われる(S11)。画質判定部3で画質が良いと判定された場合には(S12)、眼画像は眼位置検出部4に送られ、例えば前述の特許第3307936号公報に示した方法で、臉位置検出部5、極座標変換部6およびコード化部7で所定の処理が行われ、認証情報が作成される(S13)。一方、ステップS12で眼画像の画質が悪いと判定された場合には、その旨を被認証者21に対して通知し、再度眼画像の入力を行う(S10)。

[0107] 登録部20は、コード化部7からコード化された認証情報が入力された場合に、この情報を登録してよいか否かの問い合わせを管理者23に対して行う。このとき、登録部20は、コード化された認証情報と対応するコード化部7から送られた眼画像を表示画像作成部31に送り、表示画像作成部31は、第1の実施の形態で説明した表示画像作成部11と同様の方法で表示画像80の作成を行う(S14)。

[0108] そして、表示画像80は表示画像作成部31から表示部72へと送られて、表示部72は表示画像80を表示する(S15)。

[0109] 管理者23は、表示部72に表示された表示画像80を見て、その画像が登録するのに適した画像であるかの前述のような確認を行う。確認により、眼画像が登録に適当であると判断した場合には、登録許可の入力を入力部13から行う(S16)。

[0110] 登録許可の入力があった場合には(S17)、登録部20は、コード化部7から入力された認証情報を登録認証情報として記憶部9に記憶して、登録処理を終了する(S18)。一方、ステップS17において、入力部13からの入力がない場合、および画像が登録に不適当である旨の入力があった場合には、ステップS10に戻って再度眼画像を入力させてもよいし、外部の装置に対してエラー信号を発生したり、表示部72にエラーメッセージを表示したりする構成であってもよい。

[0111] 本発明の第2の実施の形態において、表示画像作成部31で眼画像の画像処理を行って表示画像80を作成する場合には、管理者23が表示部72に表示された表示

画像80を見てそれが登録してよい画像であるか否かを判定できる程度の画質が必要であり、かつ、画面コピー等で複製されてもなりすましが困難な程度の画質の画像とすることが望まれる。

- [0112] このような構成とすることにより、本発明の第2の実施の形態における認証システム70によれば、管理者23が不正な目的を持っており、表示部72に表示された表示画像80を画面コピー等して複製しても、それを用いてなりすましが困難な、セキュリティ性の高い認証システム70を実現できる。
- [0113] なお、本発明の第2の実施の形態の認証システム70においては、画像入力部62、認証装置61および表示部72が別々の機器として構成された例を示したが、本発明はこれになんら限定されるものではない。例えば、画像入力部62が認証装置61に組み込まれていたり、表示部72が認証装置61に組み込まれていたり、画像入力部62と表示部72とが一体に構成されていたり、さらには、画像入力部62、認証装置61および表示部72が一体に構成されていてもよいことはいうまでもない。
- [0114] なお、前述のように、装置が一体に構成された場合に、登録部20が認証情報を登録しようとする場合には、被認証者21自らが表示画像80を見て登録すべきか否かを判定する構成であってもよい。
- [0115] (第3の実施の形態)  
次に、本発明の第3の実施の形態における認証システム60について説明する。図12は本発明の第3の実施の形態における認証システム60の構成を示すブロック図である。
- [0116] 本発明の第3の実施の形態における認証システム60の概要は第2の実施の形態における認証システム70と同様である。ここでは説明を簡単にするために、第1の実施の形態および第2の実施の形態で説明した認証システム30および認証システム70と同様の機能ブロックについては同一の符号を付し、その説明を省略する。
- [0117] 本発明の第3の実施の形態における認証システム60が前述の認証システム70と異なるところは、認証装置75の表示画像作成部71が、登録部20に加えて眼位置検出部4および瞼位置検出部5とも接続されていることである。これにより、表示画像作成部71は、眼位置検出部4で検出された眼画像中における黒目の領域の中心位置お

および輪郭の位置(以下、眼位置と記す)および瞼位置検出部5によって検出された瞼の位置(以下、瞼位置と記す)の情報を参照して表示画像の作成処理を行うことができる。

- [0118] このような構成により、本発明の第3の実施の形態において、表示画像作成部71は、登録部20から送られた眼画像から、前述の画像圧縮、ノイズ付加、リサイズ等の処理を行った表示画像を作成できることはもちろんのこと、加えて以下の処理を行うことが可能となる。
- [0119] 以下、本発明の第3の実施の形態における表示画像作成部71の機能について、さらに詳細に説明する。
- [0120] 表示画像作成部71は、前述のように眼位置および瞼位置とを参照できるので、眼画像から認証に必要となる虹彩を含む領域を選択的に画像処理することができる。つまり、画像入力部62で入力された眼画像から、瞼位置検出部5で検出された瞼の領域を除き、眼位置検出部4で検出された黒目の領域と重なる部分を算出すれば、虹彩を含む領域を得ることが可能となる。この得られた領域について、選択的に画像処理を行えばよい。
- [0121] この表示画像作成部71が行う画像処理の一例として、図13に、黒目の領域を選択的にノイズ付加した表示画像91の例を示す。図13に示すように、全体的には、管理者23に不自然な感覚を生じさせない自然な眼画像が表示されており、管理者23はこのような表示画像91を見て、その画像を登録すべきか否かを明確に判断することがより確実に可能となる。また、表示画像91の虹彩を含む領域はノイズが付加されているので、表示画像91を用いてなりすましを試みても、認証される可能性は極めて低い。
- [0122] なお、このノイズ付加の方法は、第1の実施の形態で説明したノイズ付加方法と同じ方法を用いることが可能である。
- [0123] 次に、別の例として、図14に、眼画像の黒目の領域をあらかじめ準備した模擬虹彩のパターン図形と置換する処理を行った表示画像92の例を示す。図14に示すように、登録すべき画像の判別に用いるには十分自然で、画像の適否の判別のしやすい表示画像92を作成することが可能となる。また、なりすましをされる可能性は極めて

低いので、セキュリティ性の高い認証システム60を実現することが可能である。

- [0124] さらに、別の例として、図15に、眼画像の眼全体の領域を、あらかじめ準備したデフォルメされた眼のパターン画像と置換する画像処理を行って作成した表示画像93の例を示す。この場合には、眼位置検出部4で検出された眼の黒目領域の中心位置の座標を用いて、あらかじめ準備した所定のパターン画像と置換する。
- [0125] 表示画像93を用いた場合には、画像の登録適否の判別は、他の表示画像と比較して難しいが、第4の実施の形態で後述するような、被認証者21の誘導用に用いる場合には、問題なく使用することができるし、瞼情報を用いて、まばたきを表現するようすれば、登録可否の判別に用いることも可能となる。
- [0126] なお、上述の例では、あらかじめ準備された眼のパターン画像として、デフォルメされた眼の図形の例を示したが、本発明はこれに限定されない。
- [0127] 例えば、眼のパターン画像として、虹彩の皺パターンをあらかじめ擬似的に作成した眼画像を用意し、この眼画像を用いてもよい。
- [0128] なお、本発明の第3の実施の形態においては、表示画像作成部71と眼位置検出部4および瞼位置検出部5とがそれぞれ接続されている例を示したが、本発明はこれに限定されるものではない。例えば、接続されているのと実質的に同じ効果、例えば眼位置検出部4において検出された眼位置、および瞼位置検出部5において検出された瞼位置の情報が極座標変換部6、コード化部7および登録部20を介して表示画像作成部71に送られる構成であっても、表示画像作成部71において前述したものと同様の画像処理が可能であることはいうまでもない。
- [0129] (第4の実施の形態)
 

次に、本発明の第4の実施の形態として、本発明のさらに別の構成の認証システムについて説明する。
- [0130] 本発明の第1の実施の形態から第3の実施の形態においては、それぞれ、被認証者21の誘導を行う際に表示する画像について所定の処理を行って表示画像を作成する例として認証システム30を示し、被認証者21から撮影した眼画像を画像処理して、眼画像を登録認証画像として登録する場合における管理者23の確認用の表示画像とする例を認証システム70、60において示した。

[0131] しかしながら、本発明の認証システムはこれらの実施の形態に限定されない。

[0132] 図16は、本発明の第4の実施の形態における認証システム85の構成を示すプロック図である。本発明の第1の実施の形態から第3の実施の形態までに説明した機能ブロックと同様の機能を有する機能ブロックには、同一の符号を付し、その説明を省略する。

[0133] 本発明の第4の実施の形態における認証システム85は、第1の実施の形態で説明した認証システム30の特徴と第2の実施の形態で説明した認証システム70の特徴とを併せ持っている。

[0134] 本発明の第4の実施の形態における認証システム85の構成と、第1の実施の形態で説明した認証システム30および第2の実施の形態で説明した認証システム70との違いは、画像入力部82、表示部83および入力部84が認証装置と一体に構成されて認証システム85を形成していること、ならびに、表示画像作成部81は画像入力部82と登録部20とにそれぞれ接続されていることである。

[0135] 本発明の第4の実施の形態の認証システム85における表示画像作成部81は、前述の第1の実施の形態における認証装置1の表示画像作成部11および第2の実施の形態における認証装置61における表示画像作成部31と同様の処理、すなわち、画像全体の画像圧縮処理、ノイズ付加処理およびリサイズ処理等を行う。

[0136] このような構成とすることで、本発明の第4の実施の形態の認証システム85を用いることによって、被認証者21を誘導するために表示画像を作成して表示部83に表示できるとともに、登録部20がコード化部7から送られた認証情報を登録認証情報として記憶部9に登録しようとする場合に、管理者23(または被認証者21)に対して、確認用の表示画像を表示することができる。

[0137] これにより、被認証者21の誘導時においても、認証情報登録の確認時においても、画面コピー等されて複製されてもなりすましをされる可能性の低い画像を表示できるので、セキュリティ性の高い認証システム85を提供することができる。

[0138] (第5の実施の形態)

次に、本発明の第5の実施の形態である認証システム88について説明する。

[0139] 図17は、本発明の第5の実施の形態における認証システム88の構成を示すプロック

ク図である。

- [0140] 図17に示したように、本発明の第5の実施の形態における認証システム88は、第4の実施の形態で説明した認証システム85と共通する部分が多いが、異なる部分は、表示画像作成部94が画像入力部82や登録部20のみならず、眼位置検出部4および瞼位置検出部5それぞれと接続されていることである。
- [0141] このような構成とすることで、本発明の第5の実施の形態の認証システム88は、第1の実施の形態における認証装置1の表示画像作成部11の機能および第3の実施の形態における認証装置75の表示画像作成部71の機能を併せ持った機能を有することが可能となる。
- [0142] すなわち、認証システム88が被認証者21の誘導を行う際には、表示画像作成部94は、第1の実施の形態で説明した表示画像作成部11の機能、すなわち、画像入力部82から送られた眼画像を圧縮処理、ノイズ付加、リサイズ等することによって、複製されてもなりすましのされる可能性の少ない表示画像を表示部83に表示することが可能である。
- [0143] そして、認証システム88の登録部20が被認証者21の眼画像から作成したコード化された認証情報を記憶部9に登録させようとする場合には、表示画像作成部94は、接続された眼位置検出部4および瞼位置検出部5から虹彩を含む眼位置の情報および瞼位置の情報を得ることができるので、第3の実施の形態の認証装置75の表示画像作成部71と同様の機能、すなわち、眼の少なくとも虹彩を含む領域を選択的にノイズ付加したり、あらかじめ作成しておいた眼や図形等の画像等と置換処理したりする等が可能である。
- [0144] このような認証システム88においては、その眼位置の検出および瞼位置の検出のそれぞれの機能について、眼画像から認証情報を作成する眼位置検出部4および瞼位置検出部5の機能と共用しているので、迅速な表示画像の作成が行えるとともに、全体の装置構成や装置規模を抑制することが可能となる。
- [0145] このような構成とすることにより、本発明の第5の実施の形態の認証システム88によれば、被認証者21の誘導時には画像全体の画質を劣化させたような表示画像を用いて誘導を行うことができ、認証情報の登録時には、虹彩領域の画像は劣化してい

るもの、他の領域は劣化していないので、管理者23や被認証者がその画像を登録してよいか否かの判断がしやすい表示画像を表示することができる。

[0146] 誘導用、確認用表示画像のいずれの画像も、複製によるなりすましの可能性を著しく低下させることができるので、本発明の第5の実施の形態の認証システム88においてもセキュリティ性の高い構成を実現することができる。

[0147] なお、本発明の実施の形態においては、画像入力部、表示画像作成部および表示部が認証装置に搭載された構成を示したが、本発明はこれに限定されない。例えば、網膜認証、顔認証、動体検知等の人間の眼を含む画像を撮影して処理を行う各種装置に前述の画像入力部、表示画像作成部および表示部を導入することにより、その表示部に表示される表示画像を複製されることによる、なりすまし等の不正な行為が行われる可能性を低くすることが可能となる。

### 産業上の利用可能性

[0148] 本発明に係る眼画像入力装置および認証装置および画像処理方法ならびにプログラムによれば、画像の虹彩を含む部分の画像が劣化しているので、表示部に表示された画像を不正に取得されても、不正な者があらかじめ登録された者になります可能性が低く、セキュリティ性が高いので、眼の画像を入力する眼画像入力装置およびそれを用いた認証装置および画像処理方法ならびにプログラム等として有用である。

## 請求の範囲

- [1] 眼画像が入力される眼画像入力部と、  
前記眼画像の少なくとも虹彩を含む部分の画像を劣化させて前記眼画像の表示画像を作成する表示画像作成部と、  
前記表示画像作成部で作成された表示画像を表示する表示部とを備えたことを特徴とする眼画像入力装置。
- [2] 請求項1に記載の眼画像入力装置と、  
前記眼画像入力部から入力された被認証者の前記眼画像から、認証情報を作成する認証情報作成部と、  
前記認証情報とあらかじめ登録された登録認証情報を比較照合することにより、前記被認証者の認証を行う認証部とを備えたことを特徴とする認証装置。
- [3] 前記表示画像作成部は、前記被認証者の眼位置誘導に使用する表示画像を作成し、  
前記認証情報作成部は、前記表示部の表示画像によって所定の位置または領域まで誘導された前記被認証者の眼画像から前記認証情報を作成することを特徴とする請求項2に記載の認証装置。
- [4] 前記被認証者の眼画像から作成された認証情報を登録認証情報として登録する認証情報登録部を備え、  
前記表示画像作成部は、前記被認証者の前記眼画像の登録の可否を判定させるための表示画像を作成し、  
前記認証情報登録部は、前記表示画像作成部で作成された表示画像を前記表示部に表示させてから前記認証情報を前記登録認証情報として登録することを特徴とする請求項2に記載の認証装置。
- [5] 前記表示画像作成部は、前記眼画像の少なくとも虹彩を含む部分を選択的に画像処理して表示画像を作成することを特徴とする請求項2に記載の認証装置。
- [6] 前記認証情報作成部は、前記眼画像から眼の位置を検出する眼位置検出部と、  
前記眼画像から瞼の位置を検出する瞼位置検出部とを有し、  
前記表示画像作成部は、前記眼の位置および前記瞼の位置から前記眼画像の少な

くとも虹彩を含む部分の位置を特定し、選択的に前記画像処理を行うことを特徴とする請求項5に記載の認証装置。

- [7] 前記表示画像作成部は、前記眼画像を圧縮処理することによって表示画像を作成することを特徴とする請求項2に記載の認証装置。
- [8] 前記表示画像作成部は、前記眼画像を圧縮処理することによって表示画像を作成することを特徴とする請求項5に記載の認証装置。
- [9] 前記圧縮処理がJPEG圧縮処理であることを特徴とする請求項7に記載の認証装置
- 。
- [10] 前記圧縮処理がJPEG圧縮処理であることを特徴とする請求項8に記載の認証装置
- 。
- [11] 前記表示画像作成部は、前記眼画像を構成する画素列の間引き処理によって表示画像を作成することを特徴とする請求項2に記載の認証装置。
- [12] 前記表示画像作成部は、前記眼画像を構成する画素列の間引き処理によって表示画像を作成することを特徴とする請求項5に記載の認証装置。
- [13] 前記表示画像作成部は、前記眼画像に所定のノイズを付加する処理によって表示画像を作成することを特徴とする請求項2に記載の認証装置。
- [14] 前記表示画像作成部は、前記眼画像に所定のノイズを付加する処理によって表示画像を作成することを特徴とする請求項5に記載の認証装置。
- [15] 前記表示画像作成部は、前記眼画像を構成する画素列の間引き処理、前記眼画像の圧縮処理、および、前記眼画像に所定のノイズを付加する処理のうち少なくとも2つを組み合わせた画像処理を前記眼画像に対して行って表示画像を作成することを特徴とする請求項2に記載の認証装置。
- [16] 前記表示画像作成部は、前記眼画像を構成する画素列の間引き処理、前記眼画像の圧縮処理、および、前記眼画像に所定のノイズを付加する処理のうち少なくとも2つを組み合わせた画像処理を前記眼画像に対して行って表示画像を作成することを特徴とする請求項5に記載の認証装置。
- [17] 前記表示画像作成部は、前記眼画像の少なくとも虹彩を含む部分と所定の画像との置換処理によって表示画像を作成することを特徴とする請求項5に記載の認証装置

。

[18] 前記眼画像入力部に入力された眼画像の画質の良否を判定する画質判定部を備え  
、  
前記認証情報作成部は、前記画質判定部において画質が良いと判定された眼画像について前記認証情報を作成することを特徴とする請求項2に記載の認証装置。

[19] 被認証者の眼画像が入力される眼画像入力部と、  
前記被認証者の眼画像から認証情報を作成する認証情報作成部と、  
前記認証情報を登録認証情報として登録する認証情報登録部と、  
前記認証情報とあらかじめ登録された登録認証情報とを比較照合することにより、前記被認証者の認証を行う認証部と、  
前記眼画像の少なくとも虹彩を含む部分の画像を劣化させて表示画像を作成する表示画像作成部と、  
前記表示画像を表示する表示部とを備え、  
前記表示画像作成部は、前記被認証者の誘導を行う場合および前記認証情報登録部が前記認証情報を前記登録認証情報として登録する場合の少なくともいずれかの場合に前記表示画像を作成して前記表示部に表示させることを特徴とする認証装置  
。

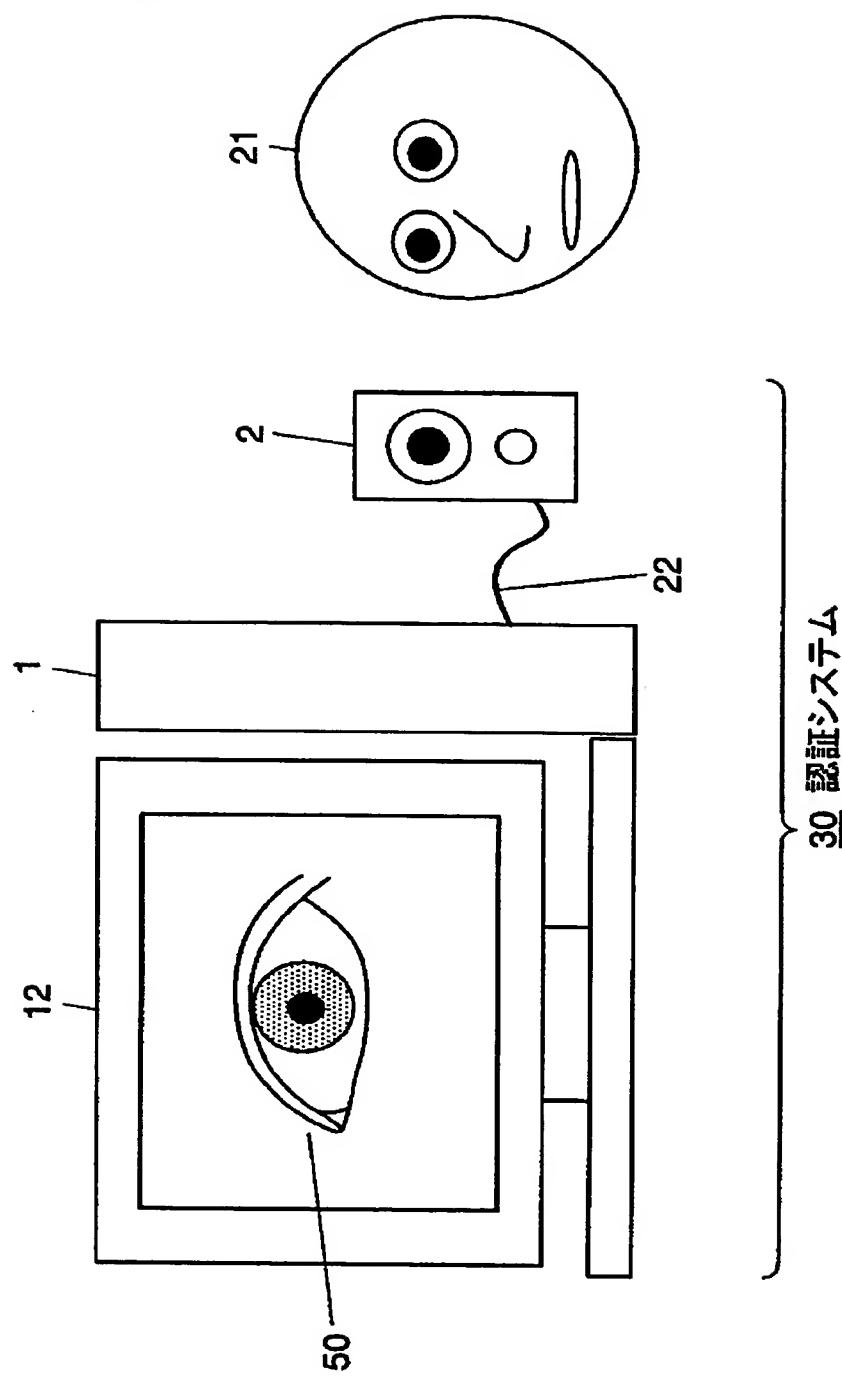
[20] 眼画像から少なくとも虹彩を含む領域を切出す第1のステップと、  
前記第1のステップで切出された前記領域の画像を選択的に劣化させる処理を行う第2のステップとを備えたことを特徴とする画像処理方法。

[21] コンピュータに、  
眼画像から少なくとも虹彩を含む領域を切出す第1のステップと、  
前記第1のステップで切出された前記領域の画像を選択的に劣化させる処理を行う第2のステップとを実行させることを特徴とするプログラム。

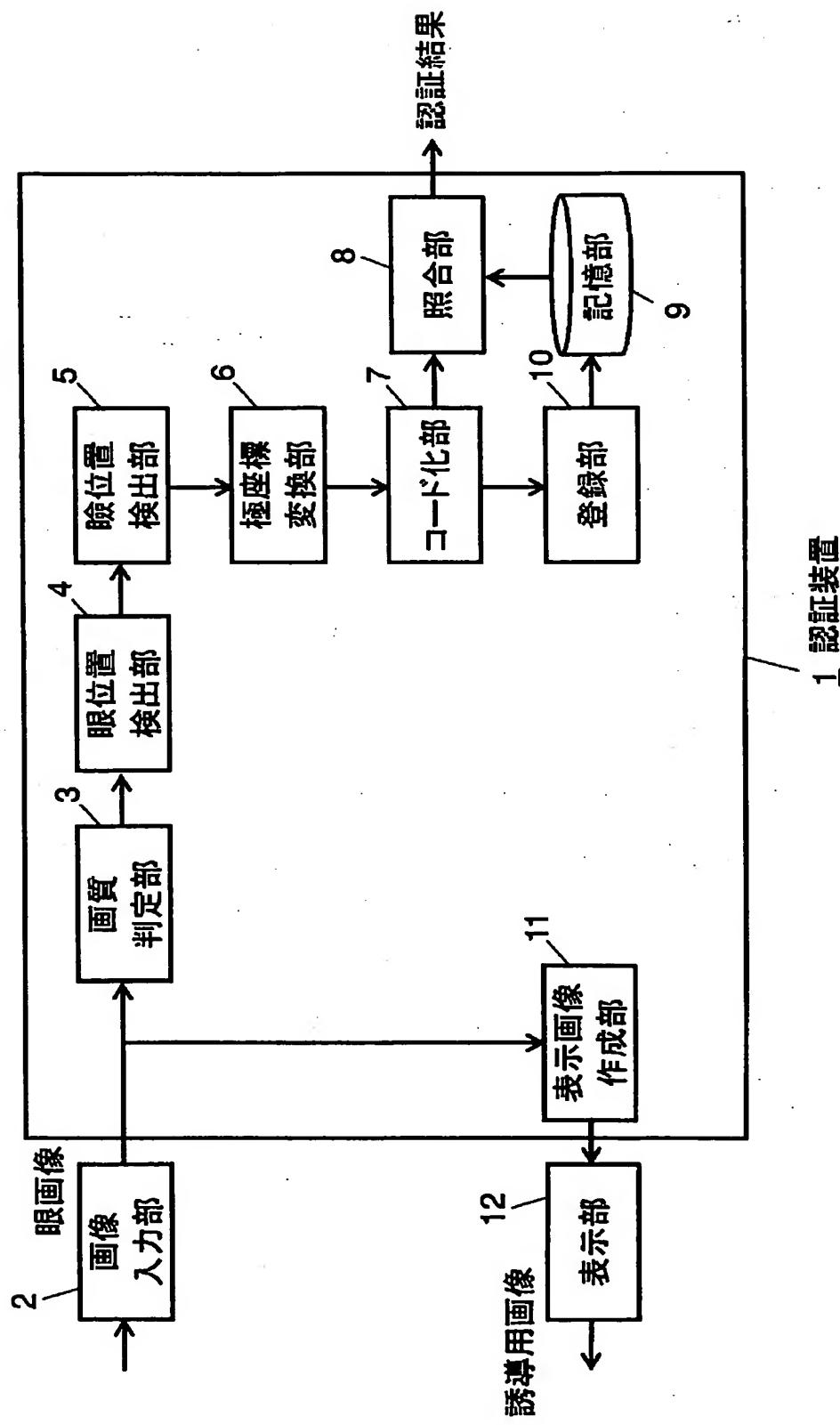
## 要 約 書

本発明の眼画像入力装置は、眼画像が入力される眼画像入力部と、眼画像の少なくとも虹彩を含む部分の画像を劣化させて認証に使用するには極めて困難な画質の表示画像を作成する表示画像作成部と、表示画像を表示する表示部とを備えた。

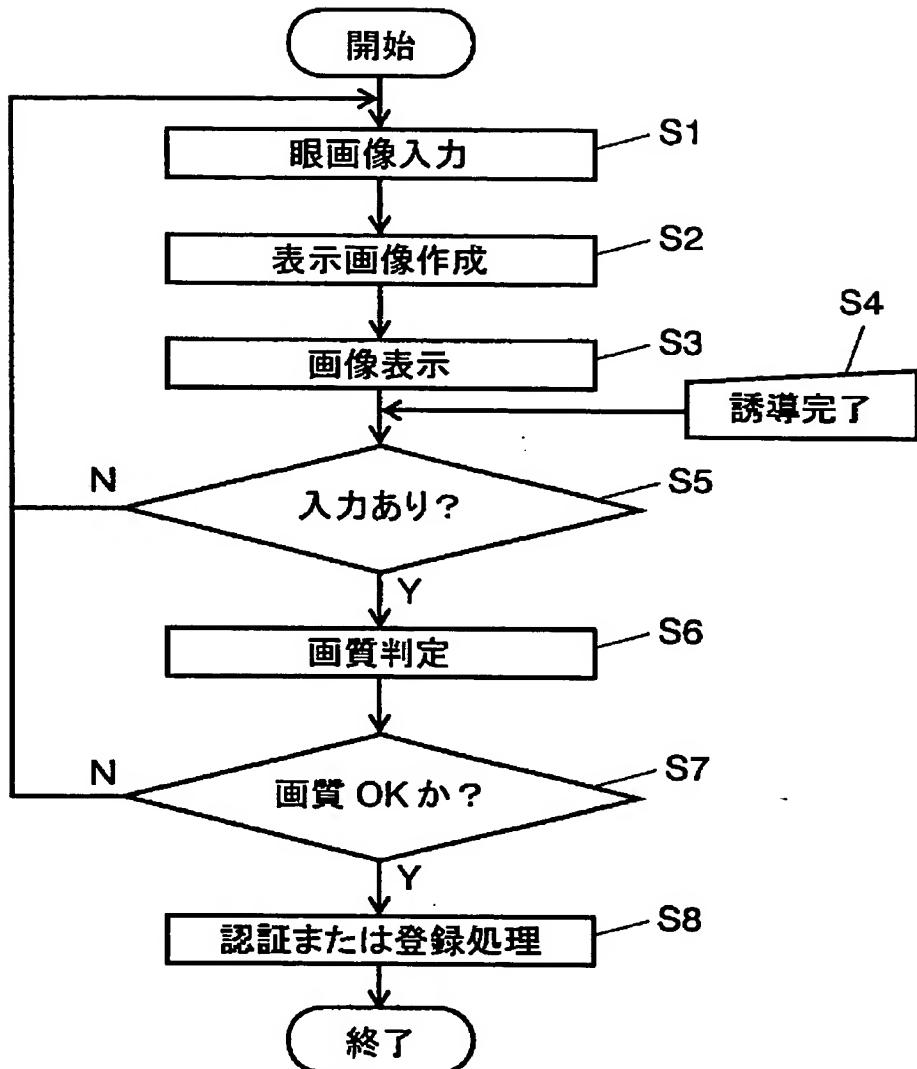
[図1]



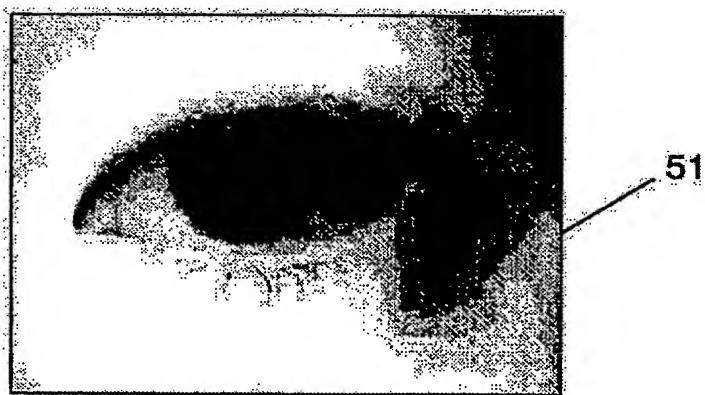
[図2]



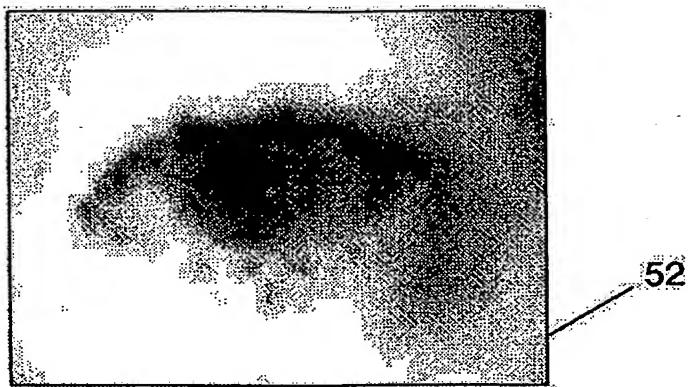
[図3]



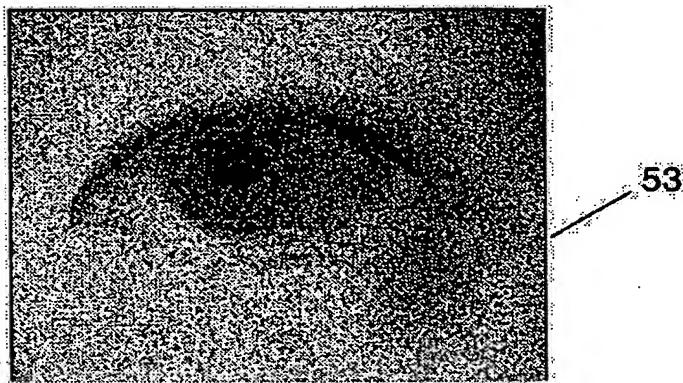
[図4]



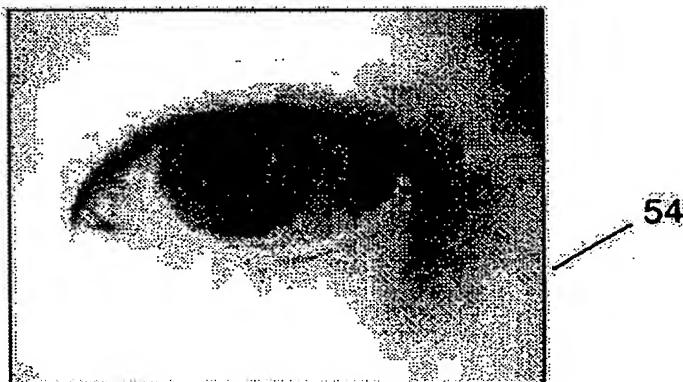
[図5]



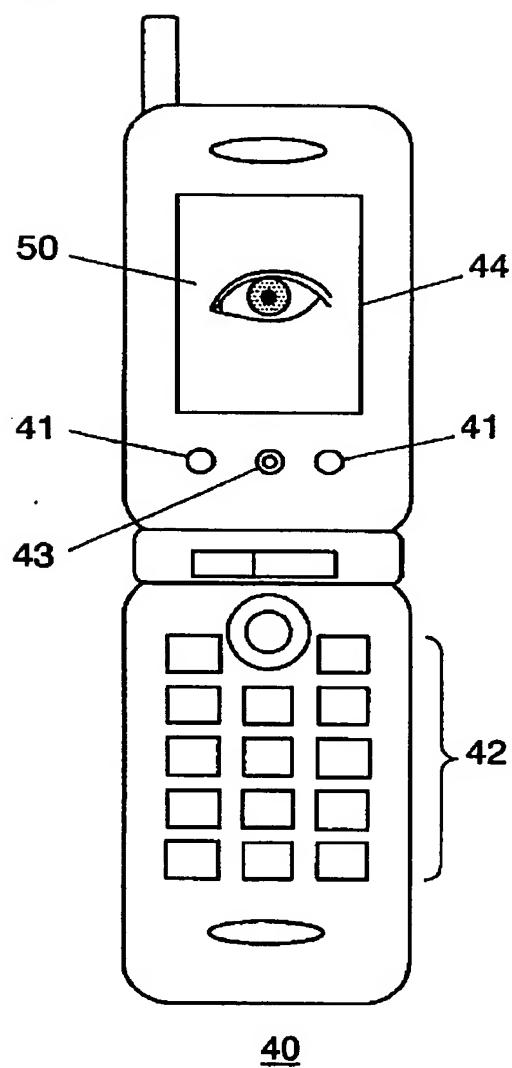
[図6]



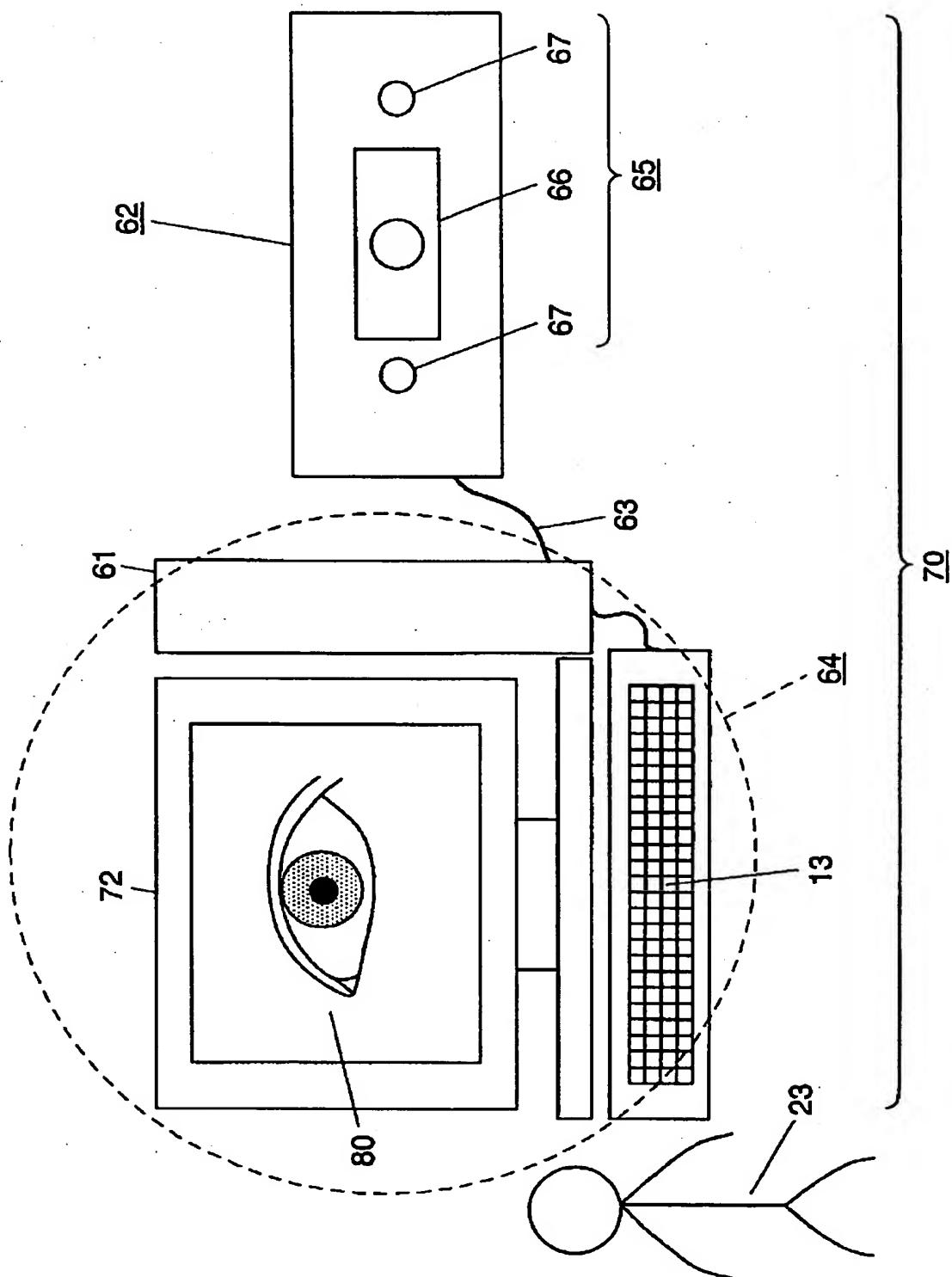
[図7]



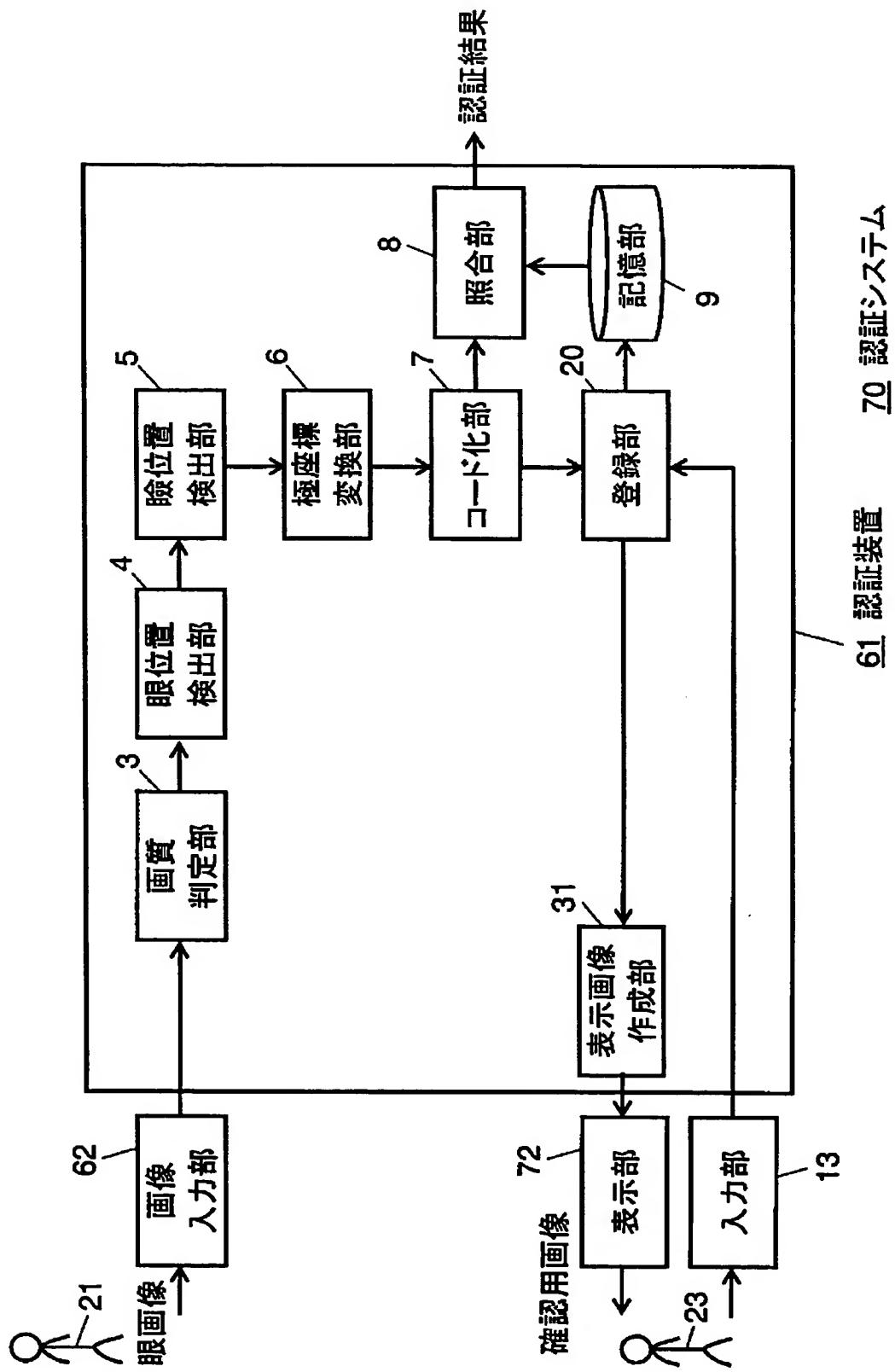
[図8]



[図9]



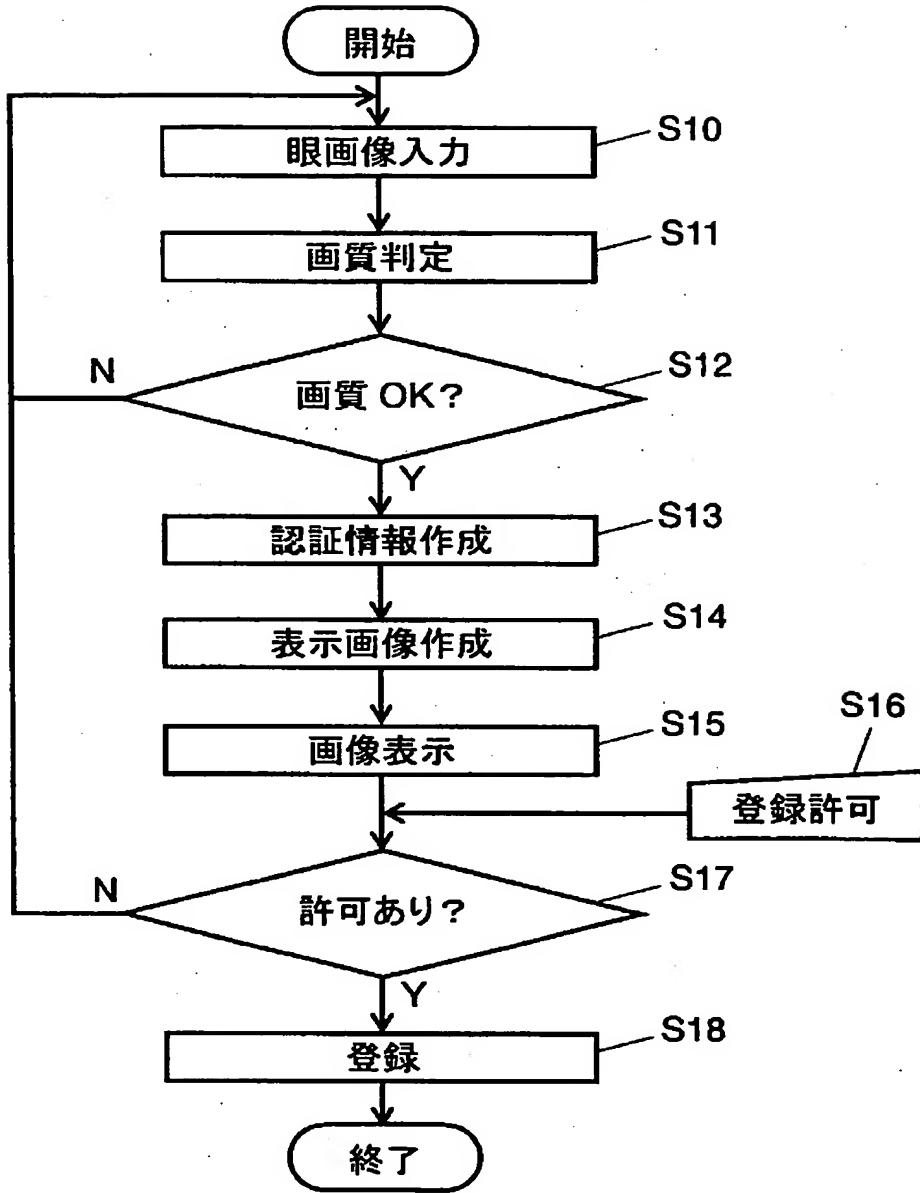
[図10]



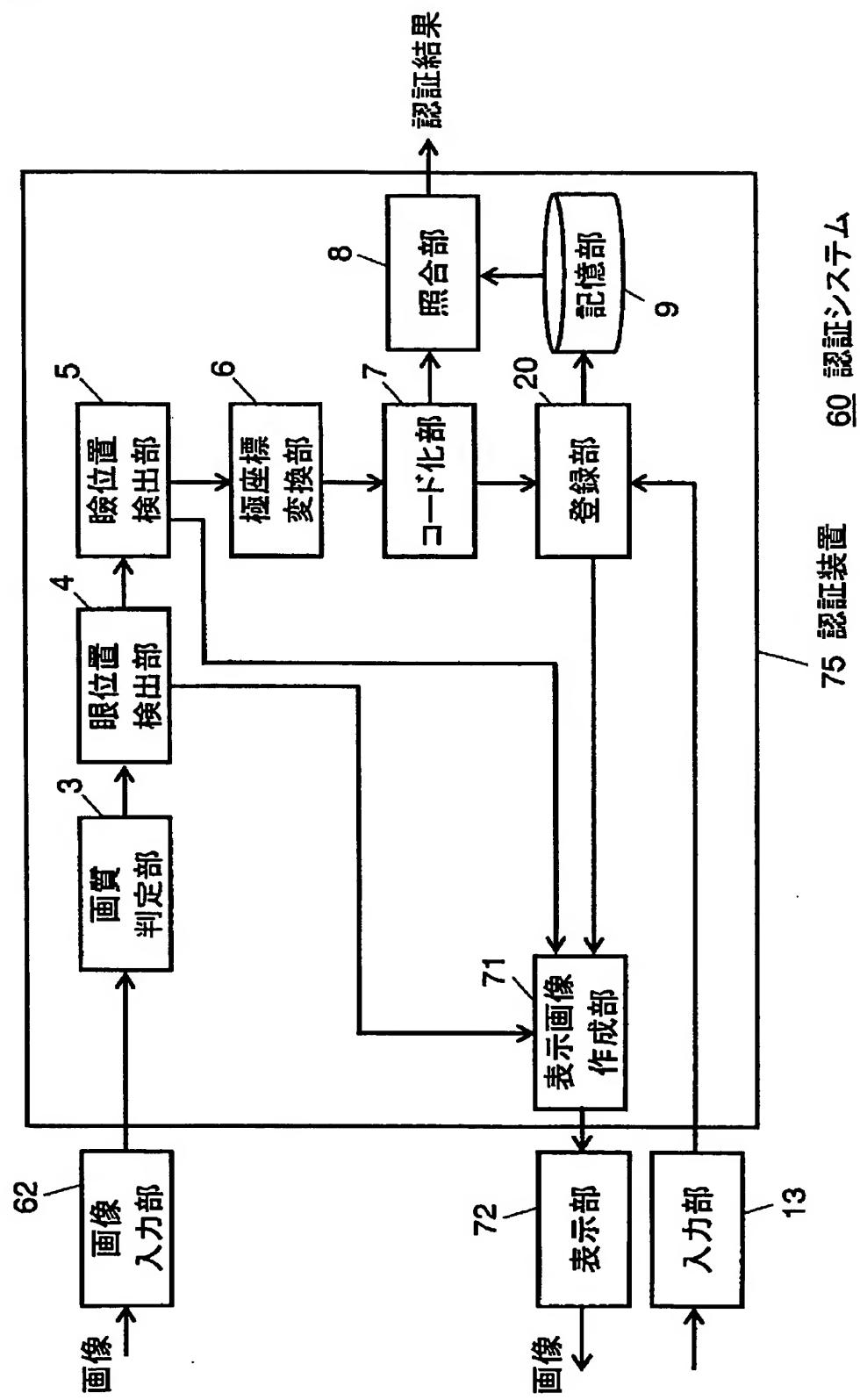
61 認証装置    70 認証システム

13

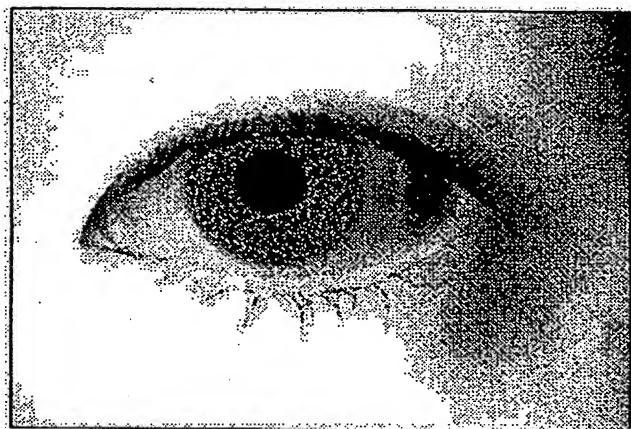
[図11]



[図12]

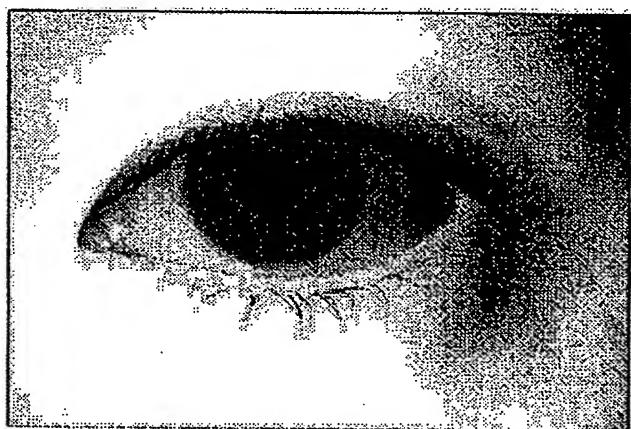


[図13]



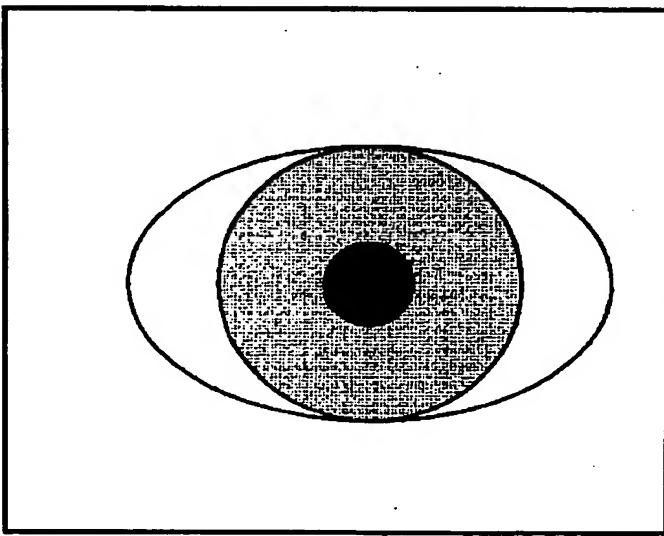
91

[図14]



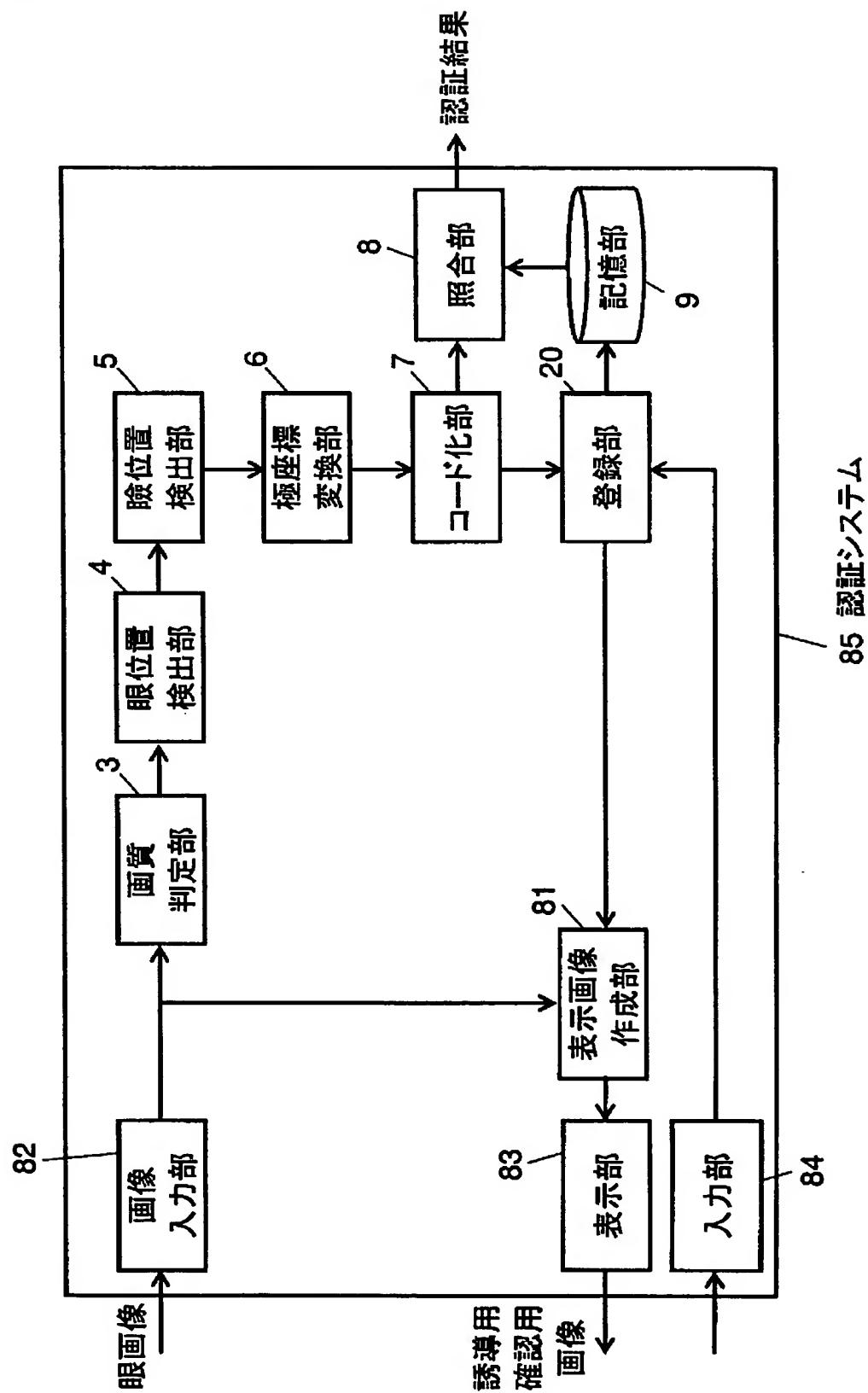
92

[図15]



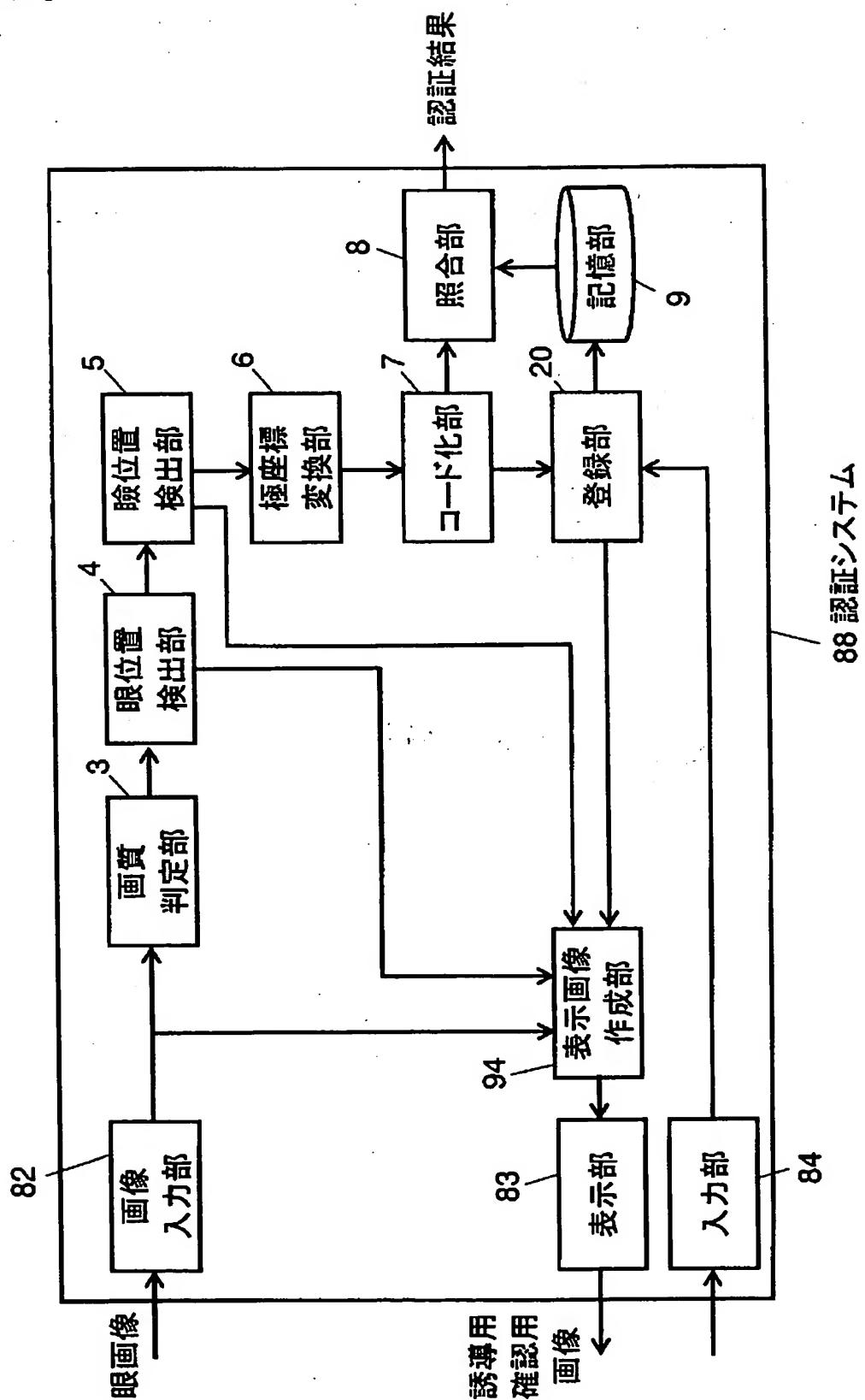
93

[図16]



85 認証システム

[図17]



THIS PAGE BLANK (USPTO)